

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

JP979 U.S. PRO
09/770397
01/29/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出願年月日
Date of Application:

2000年 2月 3日

出願番号
Application Number:

特願2000-032699

出願人
Applicant(s):

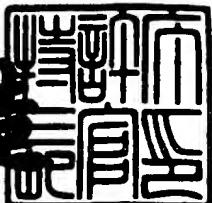
ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月 8日

特許庁長官
Commissioner,
Patent Office

及川耕造



出許番号 出許特2000-3102203

【書類名】 特許願
【整理番号】 9900738506
【提出日】 平成12年 2月 3日
【あて先】 特許庁長官 近藤 隆彦 殿
【国際特許分類】 G11B 20/12
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 千秋 進
【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之
【代理人】
【識別番号】 100067736
【弁理士】
【氏名又は名称】 小池 晃
【選任した代理人】
【識別番号】 100086335
【弁理士】
【氏名又は名称】 田村 篤一
【選任した代理人】
【識別番号】 100096677
【弁理士】
【氏名又は名称】 伊賀 誠司
【手数料の表示】
【予納台帳番号】 019530
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システム

【特許請求の範囲】

【請求項1】 記録媒体にデジタルデータを記録するデータ記録方法において、

上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成し、

上記デジタルデータのデータ識別情報及びデータ制御情報を上記記録識別情報を用いて暗号化し、

少なくともこの暗号化されて得られた暗号化データと上記記録識別情報を上記記録媒体に記録すること

を特徴とするデータ記録方法。

【請求項2】 上記デジタルデータは上記データ識別情報により暗号化されており、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体に記録することを特徴とする請求項1記載のデータ記録方法。

【請求項3】 上記データ制御情報には、上記デジタルデータのコピー制御情報が含まれていることを特徴とする請求項1記載のデータ記録方法。

【請求項4】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を、上記記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記記録媒体に記録することを特徴とする請求項1記載のデータ記録方法。

【請求項5】 上記データ識別情報及びデータ制御情報の暗号化を行うデータ処理部と上記記録媒体にデータを記録するデータ記録部とが分離して設けられ、上記データ記録部で上記記録識別情報を生成すると共に、この生成された記録識別情報を暗号化して上記データ処理部に送ることを特徴とする請求項1記載のデータ記録方法。

【請求項6】 記録媒体にデジタルデータを記録するデータ記録装置において、

上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成する手段

と、

上記ディジタルデータのデータ識別情報及びデータ制御情報を上記記録識別情報用いて暗号化する手段と、

少なくともこの暗号化されて得られた暗号化データと上記記録識別情報を上記記録媒体に記録する手段と

を有して成ることを特徴とするデータ記録装置。

【請求項7】 上記ディジタルデータは上記データ識別情報により暗号化されており、この暗号化されたディジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体に記録することを特徴とする請求項6記載のデータ記録装置。

【請求項8】 上記データ制御情報には、上記ディジタルデータのコピー制御情報が含まれていることを特徴とする請求項6記載のデータ記録装置。

【請求項9】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を、上記記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記記録媒体に記録することを特徴とする請求項6記載のデータ記録装置。

【請求項10】 ディジタルデータのデータ識別情報及びデータ制御情報の暗号化を行うデータ処理装置と、このデータ処理装置からの暗号化データを記録媒体に記録するデータ記録再生装置とを有するデータ記録再生システムであって、

上記データ記録再生装置は、上記ディジタルデータの記録毎にそれぞれ独立の記録識別情報を生成する手段と、上記データ処理部からのデータと上記記録識別情報を上記記録媒体に記録する手段とを有し、

上記データ処理装置は、上記データ記録再生装置からの上記記録識別情報を用いて、上記ディジタルデータのデータ識別情報及びデータ制御情報を暗号化し、上記データ記録再生装置に送る

ことを特徴とするデータ記録再生システム。

【請求項11】 上記ディジタルデータは上記データ識別情報により暗号化されており、上記データ記録再生装置は、この暗号化されたディジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体に記録することを特徴とする請求項10記載のデータ記録

再生システム。

【請求項12】 上記データ制御情報には、上記ディジタルデータのコピー制御情報が含まれていることを特徴とする請求項10記載のデータ記録再生システム。

【請求項13】 上記データ記録再生装置は、上記データ処理装置からの上記暗号化された上記データ識別情報及びデータ制御情報並びに上記記録識別情報を、上記記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記記録媒体に記録することを特徴とする請求項10記載のデータ記録再生システム。

【請求項14】 上記データ記録再生装置は、上記記録識別情報を上記データ処理装置に送る際に認証処理を行い、上記データ処理装置が正当であると認証されたとき、上記記録識別情報を暗号化して上記データ処理装置に送ることを特徴とする請求項10記載のデータ記録再生システム。

【請求項15】 記録媒体にディジタルデータを再生するデータ再生方法において、

上記記録媒体から記録識別情報を用いて暗号化されたデータ識別情報及びデータ制御情報の暗号化データと記録識別情報とを再生し、

上記データ識別情報及びデータ制御情報の暗号化データを上記記録識別情報を用いて復号し、上記データのデータ識別情報及びデータ制御情報を取り出すことを特徴とするデータ再生方法。

【請求項16】 上記ディジタルデータは上記データ識別情報により暗号化されて上記記録媒体に記録されており、この暗号化されたディジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体から再生することを特徴とする請求項15記載のデータ再生方法。

【請求項17】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報は、上記記録媒体に固有の記録媒体識別情報を用いて暗号化されて上記記録媒体に記録されており、上記記録媒体から上記固有の記録媒体識別情報を再生し、この再生された上記固有の記録媒体識別情報を用いて、該固有の記録媒体識別情報にて暗号化されたデータを復号し、上記データ識別情報及び

データ制御情報の暗号化データ並びに上記記録識別情報を取り出すことを特徴とする請求項15記載のデータ再生方法。

【請求項18】 上記データ識別情報及びデータ制御情報の暗号化を行うデータ処理部と上記記録媒体にデータを記録するデータ記録部とが分離して設けられ、上記データ記録部で上記記録識別情報を生成すると共に、この生成された記録識別情報を暗号化して上記データ処理部に送ることを特徴とする請求項15記載のデータ再生方法。

【請求項19】 記録媒体からデジタルデータを再生するデータ再生装置において、

上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を用いて暗号化された上記デジタルデータのデータ識別情報及びデータ制御情報をの暗号化データと上記記録識別情報を上記記録媒体から再生する手段と、

上記データ識別情報及びデータ制御情報の暗号化データを上記記録識別情報を用いて復号し、上記データ識別情報及びデータ制御情報を取り出す手段とを有して成ることを特徴とするデータ再生装置。

【請求項20】 上記デジタルデータは上記データ識別情報により暗号化されて上記記録媒体に記録されており、この暗号化されたデジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体から再生することを特徴とする請求項19記載のデータ再生装置。

【請求項21】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報は、上記記録媒体に固有の記録媒体識別情報を用いて暗号化されて上記記録媒体に記録されており、上記記録媒体から上記固有の記録媒体識別情報を再生し、この再生された上記固有の記録媒体識別情報を用いて、該固有の記録媒体識別情報にて暗号化されたデータを復号し、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を取り出すことを特徴とする請求項20記載のデータ再生方法。

【請求項22】 記録媒体からデジタルデータの記録毎にそれぞれ独立の記録識別情報を用いて暗号化されたデータを再生するデータ記録再生装置と、暗号

化されたデータを復号してディジタルデータのデータ識別情報及びデータ制御情報を取り出すデータ処理装置とを有するデータ記録再生システムであって、

上記データ記録再生装置は、上記記録識別情報と上記暗号化されたデータとを上記記録媒体から再生する手段と、これらのデータを上記データ処理装置へ送る手段とを有し、

上記データ処理装置は、上記データ記録再生装置からの上記記録識別情報を用いて上記暗号化されたデータを復号し、上記ディジタルデータのデータ識別情報及びデータ制御情報を取り出す

ことを特徴とするデータ記録再生システム。

【請求項23】 上記ディジタルデータは上記データ識別情報により暗号化されて上記記録媒体に記録されており、上記データ記録再生装置は、この暗号化されたディジタルデータを、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報と共に、上記記録媒体から再生することを特徴とする請求項22記載のデータ記録再生システム。

【請求項24】 上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報は、上記記録媒体に固有の記録媒体識別情報を用いて暗号化されて上記記録媒体に記録されており、上記記録媒体から上記固有の記録媒体識別情報を再生し、この再生された上記固有の記録媒体識別情報を用いて、該固有の記録媒体識別情報にて暗号化されたデータを復号し、上記データ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を取り出すことを特徴とする請求項22記載のデータ記録再生システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムに関し、特に、ディスク状記録媒体における不正なディスクコピーを防止するのに好適なデータ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムに関するものである。

【0002】

【従来の技術】

ディスク等の記録媒体に記録されたデジタルコンテンツデータ等のデータを他の記録媒体にコピーすることは、著作権の保護等を勘案して、自由にあるいは制限付きで行えたり、完全に禁止される場合があるが、制限付きコピーやコピー禁止の場合には、何らかのデータ保護対策が必要とされる。ここで、上記コンテンツデータには、例えば、音楽、映像、プログラムやテキスト等の著作物が挙げられる。また、ディスク等の記録媒体のコピーを防ぐ方法としては、記録媒体の識別情報（ID）を用いてコンテンツやコンテンツ鍵を暗号化する方法等が提案されている。

【0003】

【発明が解決しようとする課題】

ところで、記録すべきコンテンツデータを処理するデータ処理部と、データをディスク等の記録媒体に記録する記録部とが、同一装置内、同一基板上あるいは同一チップ内で一体化されている場合には、お互いのインターフェースから外部にデータが出なければディスクコピーを防止することができる。

【0004】

しかしながら、データ処理部と記録部とが個別の装置に分離されて設けられ、これらの装置間を例えば一般的なインターフェースで接続した場合は、インターフェース間で伝送されるデータを外部に取り出すことができ、データコピーやディスクコピーが可能となる。

【0005】

また、データ処理部と記録部とが同一の装置内、あるいは同一の基板上に設けられている場合でも、データ処理部と記録部との間のデータ線の信号をモニタする等により、データコピーやディスクコピーが行われる可能性も存在する。

【0006】

本発明は、上述の問題点に鑑みてなされたものであって、データ処理部と記録部との間で伝送される信号をモニタされた場合に、データ解読が困難で、データコピーやディスクコピーを防止でき、有効なデータ保護が図れるようなデータ記

録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムを提供することを目的とする。

【0007】

【課題を解決するための手段】

上述の課題を解決するために、本発明は、記録媒体にデジタルデータを記録する際に、上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成し、この生成された記録識別情報を用いて上記デジタルデータのデータ識別情報及びデータ制御情報を暗号化し、少なくともこの暗号化されて得られた暗号化データと上記記録識別情報を上記記録媒体に記録することを特徴とする。

【0008】

また、本発明にかかるデータ記録再生システムは、上述の課題を解決するために、デジタルデータの暗号化を行うデータ処理装置と、このデータ処理部からの暗号化データを記録媒体に記録するデータ記録再生装置とを有するデータ記録再生システムであって、上記データ記録再生装置は、上記デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成する手段と、この生成された記録識別情報を用いて暗号化されて得られた暗号化データと上記記録識別情報を上記記録媒体に記録する手段とを有し、上記データ処理装置は、上記データ記録再生装置からの上記記録識別情報を用いて、上記デジタルデータのデータ識別情報及びデータ制御情報を暗号化し、上記データ記録再生装置に送ることを特徴としている。

【0009】

ここで、上記デジタルデータはデータ識別情報を用いて暗号化されており、上記デジタルデータのデータ識別情報及びデータ制御情報の暗号化データ並びに上記記録識別情報を記録媒体に固有の記録媒体識別情報を用いて暗号化し、上記暗号化されたデジタルデータと共に、上記記録媒体に記録することが挙げられる。

【0010】

上記記録媒体に記録された上記データ識別情報及びデータ制御情報の暗号化データと上記記録識別情報を読み出して、上記記録識別情報を用いて上記データ

識別情報及びデータ制御情報を復号する。

【0011】

【発明の実施の形態】

以下、本発明に係るデータ記録方法及び装置、データ再生方法及び装置、並びにデータ記録再生システムの実施の形態について、図面を参照しながら説明する。

【0012】

図1は、本発明の実施の形態となるデータ記録装置の一例となるディスク記録再生装置10と、このディスク記録再生装置10に接続される機器の一例としてのパーソナルコンピュータ等のデータ処理装置100の概略構成を示す図である。

【0013】

この図1において、ディスク記録再生装置10は、着脱可能な追記型光ディスクや、書き換えが可能な光磁気ディスクや相変化型ディスク等の記録媒体であるディスク30を回転駆動するスピンドルモータ11と、ディスク30に対してレーザ光を照射すると共にその戻り光を受光する光学ピックアップ12と、光学ピックアップ12のレーザダイオード等のレーザ光源を駆動するレーザドライバ13と、光学ピックアップ12から出力された信号を検出する信号検出部14と、レーザドライバ13への信号の変調や信号検出部14からの信号の復調を行う変復調部15と、データを一時記憶するバッファメモリ16と、調停部17と、エラー訂正符号化／復号処理を行うECC (Error Correction Code) 部18と、パーソナルコンピュータ等のデータ処理装置100との間でデータを入出力するI/F (インターフェース) 部19と、データ記録の度毎に異なる記録ID (識別情報) を生成する記録ID生成部20とを有して構成されている。調停部17は、バッファメモリ16と、変復調部15、ECC部18及びI/F部19との間のデータ入出力を調停し、記録ID生成部20からの記録IDは、ECC部18に送られ、また、外部のデータ処理装置100にも送られる。

【0014】

スピンドルモータ11は、図示しないサーボ回路の制御の下に、ディスク30

を一定線速度で、あるいは一定角速度で回転駆動する。

【0015】

光学ピックアップ12は、ディスク30に対するデータの記録時には、レーザドライバ13により駆動された図示しないレーザ光源からのレーザ光を対物レンズ等の光学系を介してディスク30上に照射して、データを記録する。また、光学ピックアップ12は、ディスク30に記録されているデータの再生時には、図示しないレーザ光源からのレーザ光を光学系を介してディスク30上に照射すると共に、ディスク30の表面で反射回折された戻り光を図示しないフォトダイオード等の光検出素子で受光して電気信号に変換して出力する。

【0016】

このような光学ピックアップ12によりディスク30に対してデータを記録／再生する際には、受光した戻り光の検出信号に基づいて、トラッキング制御やフォーカス制御を行うことは勿論である。

【0017】

記録ID生成部20は、記録ファイル（記録内容）に対する固有の識別情報である記録IDを生成する。この記録IDは、データファイル等を記録する毎に更新され、各記録動作に対して固有の識別情報であり、ディスク装置が同じでも、同じディスクに対しても、記録が異なれば異なる記録IDとなる。この記録IDは、例えば乱数発生器等により発生された乱数に基づいて生成すればよい。

【0018】

記録ID生成部20で生成された記録IDは、そのままデータ処理装置100に送ってもよいが、必要に応じて、暗号化・認証部21により暗号化してデータ処理装置100に送るようにしてもよい。暗号化・認証部21では、上記記録IDに対して暗号化演算j()を施して、暗号化された記録IDデータをI/F（インターフェース）部19を介してデータ処理装置100に送っている。この暗号化・認証部21は、データ処理再生装置100との間で相互認証を行う機能も有している。

【0019】

また、ディスク記録再生装置10のディスクID生成部23からは後述するデ

ディスクID（識別情報）が生成され、これがECC部18に設けられた暗号化部24に送られる。また、暗号化部24には、記録ID生成部20からの記録ID（識別情報）も送られる。

【0020】

暗号化部24は、記録しようとするデータ及び上記記録IDに対して、上記ディスクIDを用いた鍵によりそれぞれ暗号化処理 $e()$, $f()$ を施し、調停部17及びバッファメモリ16を介してECC部18に送り、また、ECC部18から調停部17及びバッファメモリ16を介して得られた再生データに対して、それぞれ上記ディスクIDを用いた鍵により暗号の復号処理 $e^{-1}()$, $f^{-1}()$ を施す。

【0021】

次に、このようなディスク記録再生装置10に接続されるパーソナルコンピュータ等のデータ処理装置100は、ディスク記録再生装置10との間でデータの入出力を行うためのI/F（インターフェース）部101と、データの暗号化及び復号（暗号解読）を行う暗号化部102と、各種データ処理を行うためのデータ処理部103と、外部の認証機関等との間で相互認証等を行うための認証部104と、外部との間でデータ識別情報（後述するコンテンツID）やデータ制御情報（例えばコピー制限や禁止等の制御情報）の入出力を行うためのI/F（インターフェース）部105と、I/F部101からの暗号化された上記記録IDを復号して暗号化部102に送る暗号化・認証部22とを有している。暗号化・認証部22は、ディスク記録再生装置10との間での相互認証を行う機能も有している。また、データ処理装置100は、コンテンツデータ系として、外部から暗号化されたコンテンツデータを入力するI/F（インターフェース）部106と、I/F部106からの暗号化コンテンツデータをコンテンツID（データ識別情報）を用いて復号するための復号部107とを有しており、コンテンツIDは、認証部104における認証等が正常に行われて正当なユーザであることが確認された場合に、データ処理部103から復号部107に送られるようになっている。

【0022】

次に、図1の構成における動作について、図2等も参照しながら説明する。

ディスク記録再生装置10に接続されるパーソナルコンピュータ等のデータ処理装置100には、認証機関や鍵配達センタ等からのコンテンツID及び制御情報がI/F部105を介して供給され、また、コンテンツ配達センタやコンテンツプロバイダ等から暗号化されたコンテンツデータがI/F部106を介して供給されるようになっている。ここで、上記コンテンツデータをu、暗号化の鍵となるコンテンツIDをcIDとし、暗号化処理をc()とするとき、暗号化コンテンツデータは、 $c(u, cID)$ と表される。また、上記制御情報をcINとし、コンテンツID cID 及び制御情報cINの暗号化処理をs()とするとき、暗号化されたコンテンツID及び制御情報は、 $s(cID+cIN)$ と表される。

【0023】

図2の例では、データ処理装置100_0からのデータをディスク記録再生装置10_0で記録することにより得られたディスク30_0を、他のディスク記録再生装置10_1で再生する場合を示している。この図2のデータ処理装置100_0には、暗号化されたコンテンツデータ $c(u_0, cID_0)$ と、暗号化されたコンテンツID及び制御情報 $s(cID_0+cIN_0)$ とが供給されている。

【0024】

データ処理装置100において、例えば認証機関との間で相互認証等を行い、正当であると判断（認証）されたデータ処理装置100には、暗号化されたコンテンツID及び制御情報 $s(cID+cIN)$ が送られる。正当なデータ処理装置100においては、上記 $s(cID+cIN)$ を復号（暗号解読）することができ、暗号化コンテンツの鍵として用いられるコンテンツID cIDを得ることができる。

【0025】

すなわち、図2の例では、データ処理装置100_0に供給された暗号化されたコンテンツID及び制御情報 $s(cID_0+cIN_0)$ に復号処理 $s^{-1}()$ を施すことで、元の暗号化前のコンテンツID及び制御情報 cID_0+cIN_0 が得られる。配信された暗号化コンテンツデータ $c(u_0, cID_0)$ は、制御情報 cIN_0 により制御される。例えば、コンテンツのコピー回数に制限がある場合に、コンテンツを記録するときには、上記制御情報 cIN_0 は例えばデータ処理部104により変更されて cIN_1 となる。この制御情報に応じて、コピー回数が制限されたりコピー禁止とされた

りする。また、上記暗号化コンテンツデータ $c(u_0, cID_0)$ は、上記復号されたコンテンツID cID_0 を用いて復号することにより元の暗号化前のコンテンツデータ u_0 を得ることができる。

【0026】

図2のディスク記録再生装置10_1では、記録を行う毎に新たな記録ID、例えば wID_0 を発生し、暗号化処理 $j()$ を施してデータ処理装置100_0に送る。図2のデータ処理装置100_0においては、ディスク記録再生装置10_1からの暗号化された記録ID $j(wID_0)$ を復号して得られた記録ID wID_0 を用いて、上記コンテンツIDと変更された制御情報 cID_0+cIN_1 を暗号化し、暗号化データ $v(cID_0+cIN_1, wID_0)$ を生成し、ディスク記録再生装置10_1に送っている。上記暗号化コンテンツデータ $c(u_0, cID_0)$ は、そのままディスク記録再生装置10_1に送っている。

【0027】

ディスク記録再生装置10_1においては、今回の記録に対応して発生された上記記録ID wID_0 を、図1のディスクID生成部23からのディスクID dID_0 を用いて暗号化処理 $f()$ を施すことにより、暗号化データ $f(wID_0, dID_0)$ を生成し、また上記コンテンツID及び制御情報の暗号化データ $v(cID_0+cIN_1, wID_0)$ に対しては、同じくディスクID dID_0 を用いて暗号化処理 $e()$ を施すことにより、暗号化データ $e(v(), dID_0)$ を生成している。なお、この $v()$ は、上記暗号化データ $v(cID_0+cIN_1, wID_0)$ を略記したものである。上記暗号化処理 $f(), e()$ については、上記ディスクID dID_0 のみならず、必要に応じて、記録単位となるブロック毎の識別情報であるブロックIDを用いるようにしてもよい。これらの暗号化データ $f(wID_0, dID_0)$ 及び $v(cID_0+cIN_1, wID_0)$ は、ディスク30_0にそれぞれ記録され、また、データ処理装置100_0からの上記暗号化コンテンツデータ $c(u_0, cID_0)$ は、そのままディスク30_0に記録される。なお、上記ディスクID dID_0 は、ディスクの初期化時やディスクの出荷時、あるいは最初の記録動作時等に、ディスク30_0上の所定領域に記録される。

【0028】

次に、記録時のディスク記録再生装置10_0とは異なるディスク記録再生装置

10_1により上記ディスク30_0を再生する場合について説明する。

【0029】

ディスク記録再生装置10_1は、上記ディスク30_0より、上記暗号化データ $e(v(), dID_0)$ 及び $f(wID_0, dID_0)$ を再生し、上記暗号化コンテンツデータ $c(u_0, cID_0)$ を再生し、またディスク30_0上の所定領域から上記ディスクID dID_0 を再生する。ディスク記録再生装置10_1内では、再生された上記暗号化データ $e(v(), dID_0)$ 及び $f(wID_0, dID_0)$ を、それぞれ上記ディスクID dID_0 を用いて復号（暗号解読）することにより、上記コンテンツID及び制御情報の暗号化データ $v(cID_0+cIN_1, wID_0)$ 及び記録ID wID_0 を得る。暗号化コンテンツデータ $v(u_0, wID_0)$ については、上記I/Fを介してデータ処理装置100_1に送り、記録ID wID_0 については、暗号化演算 $j()$ を施して、暗号化された記録IDデータ $j(wID_0)$ をデータ処理装置100_1に送る。また、上記暗号化コンテンツデータ $c(u_0, cID_0)$ は、そのままデータ処理装置100_1に送る。

【0030】

データ処理装置100_1では、暗号化された記録IDデータ $j(wID_0)$ に対し復号演算 $j^{-1}()$ を施して記録ID wID_0 を求め、この記録ID wID_0 を用いて、ディスク記録再生装置10_1からの暗号化データ $v(cID_0+cIN_1, wID_0)$ を復号（暗号解読）することにより、上記コンテンツID及び制御情報 cID_0+cIN_1 を取り出している。このコンテンツID cID_0 を用いて、上記暗号化コンテンツデータ $v(u_0, wID_0)$ を復号し、コンテンツデータ u_0 を得ることができる。このとき必要に応じて、制御情報 cIN_1 による制限を受けたり、制御情報 cIN_1 自体が変更されるような処理が行われることがある。例えば、別のディスクに再コピーする場合には、制御情報 cIN_1 が cID_2 に変更される等である。

【0031】

以上のような実施の形態によれば、ディスクID dID と記録ID wID とは無関係とすることができるため、ディスク記録再生装置10とデータ処理装置100との間以外に、ディスクID dID や記録ID wID が外部に漏洩することを防止できる。また、ディスク記録再生装置10は、コンテンツID及び制御情報の暗号化演算 $v()$ を知らないでよい。暗号化演算 $v()$ は、データ処理装置100側の責

任で行い、暗号化演算 $e()$, $f()$ は、ディスク記録再生装置10側の責任で行うことにより、ディスク記録再生装置10及びデータ処理装置100の間のインターフェースと、ディスク記録再生装置10においてディスク30に対するデータの記録再生とについての各セキュリティを独立させることができる。

【0032】

次に、図3は、上述したような記録IDを用いた暗号化を施すことによりディスクコピー防止することを説明するための図である。

【0033】

この図3において、データ処理装置100_0、100_1、及びディスク記録再生装置10_0、10_1は、上述した図2と共に説明した具体例と同様であるため、図中の対応する部分に同じ指示符号を付して説明を省略する。ただし、この図3の具体例では、データ記録再生装置10_1からの上記コンテンツID及び制御情報の暗号化データ $v(cID_0+cIN_1,wID_0)$ 及び上記暗号化コンテンツデータ $v(u_0,wID_0)$ を、他のディスク記録再生装置10_2に送って、他のディスク30_2に記録するようにしている。

【0034】

すなわち、ディスク記録再生装置10_1は、ディスク30_0を再生すること上で上記暗号化データ $f(wID_0,dID_0)$ 及び $e(v(),dID_0)$ を得、ディスク30_0の所定位置に書き込まれた上記ディスクID dID_0 を用いて復号（暗号解読）することにより、上記コンテンツID及び制御情報の暗号化データ $v(cID_0+cIN_1,wID_0)$ 及び記録ID wID_0 を得る。また、ディスク30_0を再生することにより上記暗号化コンテンツデータ $c()$ 、すなわち、 $c(u_0,cID_0)$ を得る。このディスク記録再生装置10_1から得られた上記暗号化データ $v(cID_0+cIN_1,wID_0)$ 及び暗号化コンテンツデータ $c()$ を、そのまま他のディスク記録再生装置10_2に送って、他のディスク30_2に記録する。ディスク記録再生装置10_2は、ディスク30_2に対応するディスクID dID_2 を発生してディスク30_2の所定位置に記録すると共に、データ記録の際に記録ID wID_2 を発生し、この記録ID wID_2 と上記暗号化データ $v(cID_0+cIN_1,wID_0)$ とを、ディスクID dID_2 を用いた鍵により暗号化し、得られた暗号化データ $e(v(),dID_2)$ 及び $f(wID_2,dID_2)$ をディ

スク30_2に記録する。

【0035】

このディスク30_2を、ディスク記録再生装置10_3で再生する場合には、上記ディスク記録再生装置10_2に記録された暗号化データe(v(),dID_2)及びf(wID_2,dID_2)が再生されてディスク記録再生装置10_3に送られる。また、ディスク30_2から上記暗号化コンテンツデータc()が再生されてディスク記録再生装置10_3に送られる。ディスク記録再生装置10_3では、ディスク30_2の所定位置に記録されたディスクID dID_2を読み取って、このディスクID dID_2を暗号鍵として用いることにより、上記暗号化データe(v(),dID_2)及びf(wID_2,dID_2)の復号（暗号解読）を行う。これにより、上記コピーされた暗号化データv(cID_0+cIN_1,wID_0)と、この暗号化データv(cID_0+cIN_1,wID_0)をディスク30_2で記録した際の記録ID wID_2が復元され、暗号化データv(cID_0+cIN_1,wID_0)はそのまま、記録ID wID_2は暗号化演算j()が施されて、それぞれデータ処理装置100_3に送られる。データ処理装置100_3では、暗号化された記録ID j(wID_2)に対して復号演算j⁻¹()を施して記録ID wID_2を求め、この記録ID wID_2を用いてディスク記録再生装置10_3からの暗号化データv(cID_0+cIN_1,wID_0)を復号（暗号解読）しようとするが、暗号化データv(cID_0+cIN_1,wID_0)は記録ID wID_0を鍵として用いて暗号化されたものであるため、暗号化データv(cID_0+cIN_1,wID_0)を復号して元のデータ、すなわちコンテンツID及び制御情報のデータcID_0+cIN_1を得ることができない。

【0036】

すなわち、データ処理装置100_3においては、記録ID wID_2が返されたが、暗号化データv(cID_0+cIN_1,wID_0)は記録ID wID_0により暗号化されており、その矛盾から不正にディスクコピーされたことが分かる。また、暗号化データv(cID_0+cIN_1,wID_0)は記録ID wID_2では復号されないため、元のコンテンツID及び制御情報のデータcID_0+cIN_1を得ることはできない。

【0037】

なお、上記ディスクコピーの際に、元の記録を行ったディスク記録再生装置10_0を用いて、ディスク記録再生装置10_1からの再生データをそのまま記録す

ることも考えられるが、記録（コピー）の際に新たな記録IDが生成され、この記録IDは上記元の記録時の記録ID wID_0とは異なるものとなり、この場合も復号が行えないことになる。

【0038】

次に、図4は、上記記録IDを暗号化せずにディスク記録再生装置10から対応するデータ処理装置100に送る場合を示している。これ以外は、上記図2と同様であるため、対応する部分に同じ指示符号を付して説明を省略する。

【0039】

次に、図5は、ディスク記録再生装置10とデータ処理装置100との間で、上記記録IDのみならず、コンテンツID及び制御情報の暗号化データv(cID_0+cIN_1,wID_0)についても暗号化を施して伝送する場合の例を示している。

【0040】

すなわち、記録の際には、ディスク記録再生装置10_1で発生された記録ID wID_0に暗号化処理j()を施して得られた暗号化データj(wID_0)をデータ処理装置100_0に送り、データ処理装置100_0では、この暗号化データj(wID_0)を復号して得られた記録ID wID_0を用いて、上記コンテンツIDと制御情報のデータ cID_0+cIN_1を暗号化し、暗号化データv(cID_0+cIN_1,wID_0)を生成し、さらにこの暗号化データv(cID_0+cIN_1,wID_0)に対して暗号化処理j()を施して、ディスク記録再生装置10_1に送っている。

【0041】

また、再生時には、ディスク記録再生装置10_1は、ディスク30_0を再生して得られた上記暗号化データe(v(),dID_0)及びf(wID_0,dID_0)を、同じくディスク30_0から再生されたディスクID dID_0を用いて復号することにより、上記記録ID wID_0及び暗号化データv(cID_0+cIN_1,wID_0)を求め、これらのデータ wID_0及びv(cID_0+cIN_1,wID_0)に対して、それぞれ暗号化処理j()を施し、得られた暗号化データj(wID_0)及びj(v())をデータ処理装置100_0に送っている。データ処理装置100_0では、これらの暗号化データj(wID_0)及びj(v())に対して復号処理j⁻¹()を施して、wID_0及びv(cID_0+cIN_1,wID_0)を得ている。

【0042】

この図5の例における他の構成及び動作は、上述した図2の例と同様であるため、対応する部分に同じ指示符号を付して説明を省略する。

【0043】

なお、本発明は、上述した実施の形態のみに限定されるものではなく、例えば上記実施の形態では、データ処理装置とディスク記録再生装置とを個別の装置として説明したが、同一筐体内の別基板、あるいは同一基板上の別回路部としたデータ処理部とデータ記録再生部の場合にも適用できる。また、記録媒体は、ディスク状記録媒体に限定されず、カード状やテープ状の記録媒体等にも適用できる。また、ユーザデータとしては、暗号化されていない平文のデータを用いてもよいが、既に他の暗号鍵により暗号化されているデータを用いてもよい。さらに、上記記録IDのみならず、ディスク等の記録媒体毎に固有の記録媒体ID（ディスクID等）や、符号化単位あるいは記録単位となるブロック（セクタ、フレーム等）毎に異なるブロックIDを用いるようにしてもよく、この場合、これらの記録ID、ディスクID、ブロックIDを生成するための乱数発生器等を共通化するようにしてもよい。この他、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。

【0044】**【発明の効果】**

本発明によれば、デジタルデータの記録毎にそれぞれ独立の記録識別情報を生成し、この生成された記録識別情報を用いて、上記デジタルデータのデータ識別情報及びデータ制御情報を暗号化し、少なくともこの暗号化されて得られた暗号化データと記録識別情報を記録媒体に記録することにより、記録毎に固有の記録識別情報を用いた暗号化が施されるため、記録媒体からの再生データをそのままコピーしても、データ識別情報の解読（暗号化の復号）が行えず、コピー防止が有効に行える。

【0045】

ここで、上記デジタルデータは上記データ識別情報を用いて暗号化されており、該データ識別情報が復号できない限り、暗号化コンテンツデータの復号が行

えない。

【0046】

また、上記デジタルデータの暗号化を行うデータ処理部と上記記録媒体にデータを記録するデータ記録部とを分離して設けた場合に、データ処理部とデータ記録部との間のデータをモニタされても、データ識別情報の解読が行えず、不正コピーの防止が有効に行える。

【図面の簡単な説明】

【図1】

本発明の実施の形態が適用されるディスク記録再生装置及びデータ処理装置の概略構成を示すブロック図である。

【図2】

暗号化データを記録したディスクを他のディスク記録再生装置で再生する場合を説明するための図である。

【図3】

暗号化データを記録したディスクをコピーしたディスクを再生する場合の一例を説明するための図である。

【図4】

記録識別情報をデータを暗号化しないで伝送する場合を説明するための図である。

【図5】

記録識別情報を暗号化してディスク記録再生装置からデータ処理装置に伝送すると共に暗号化されたデータ識別情報及びデータ制御情報を暗号化してデータ処理装置からディスク記録再生装置に伝送する場合を説明するための図である。

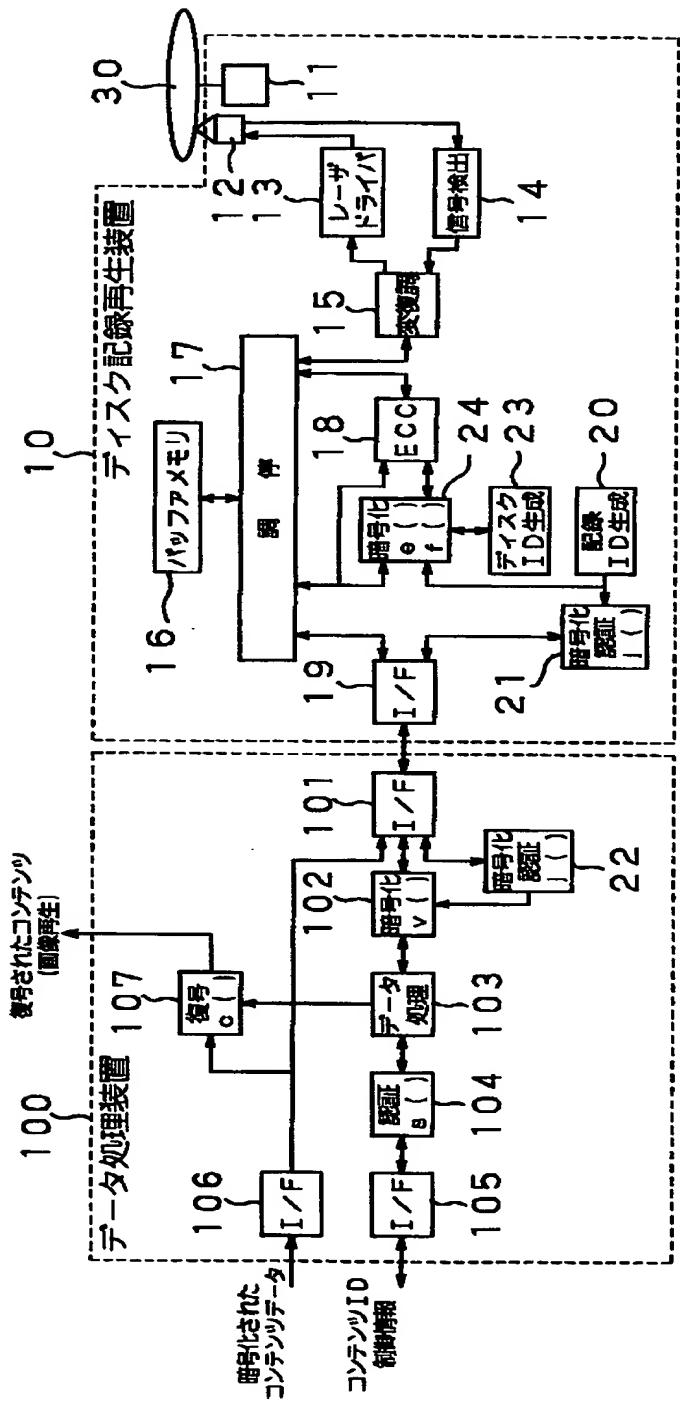
【符号の説明】

10 ディスク記録再生装置、 15 変復調部、 16 バッファメモリ、
17 調停部、 18 ECC部、 19, 101, 105, 106 I/F
(インターフェース) 部、 20 記録ID生成部、 21, 22 暗号化・認証部、
24, 102 暗号化部、 100 データ処理装置、 103 データ処理部、
107 復号部

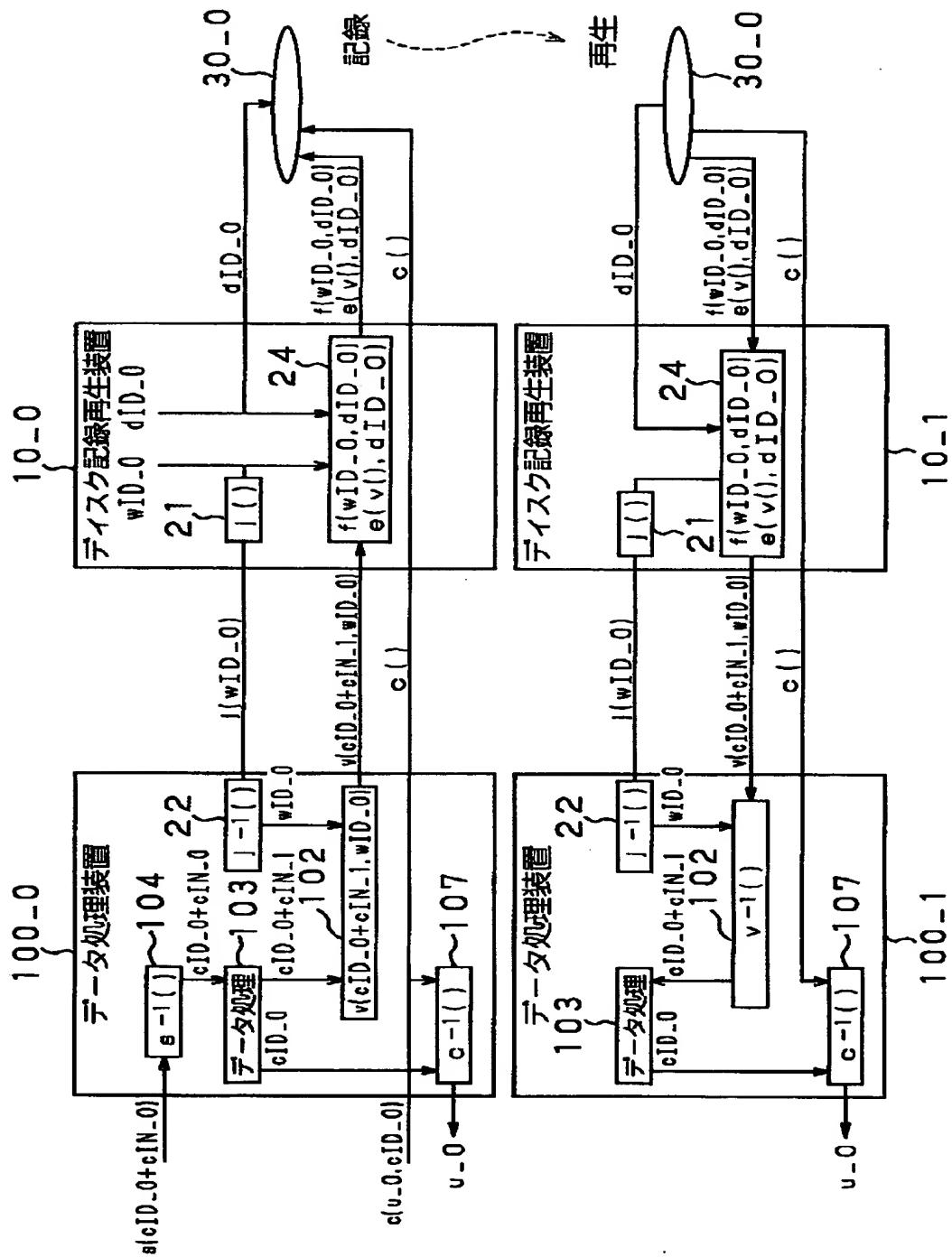
【書類名】

図面

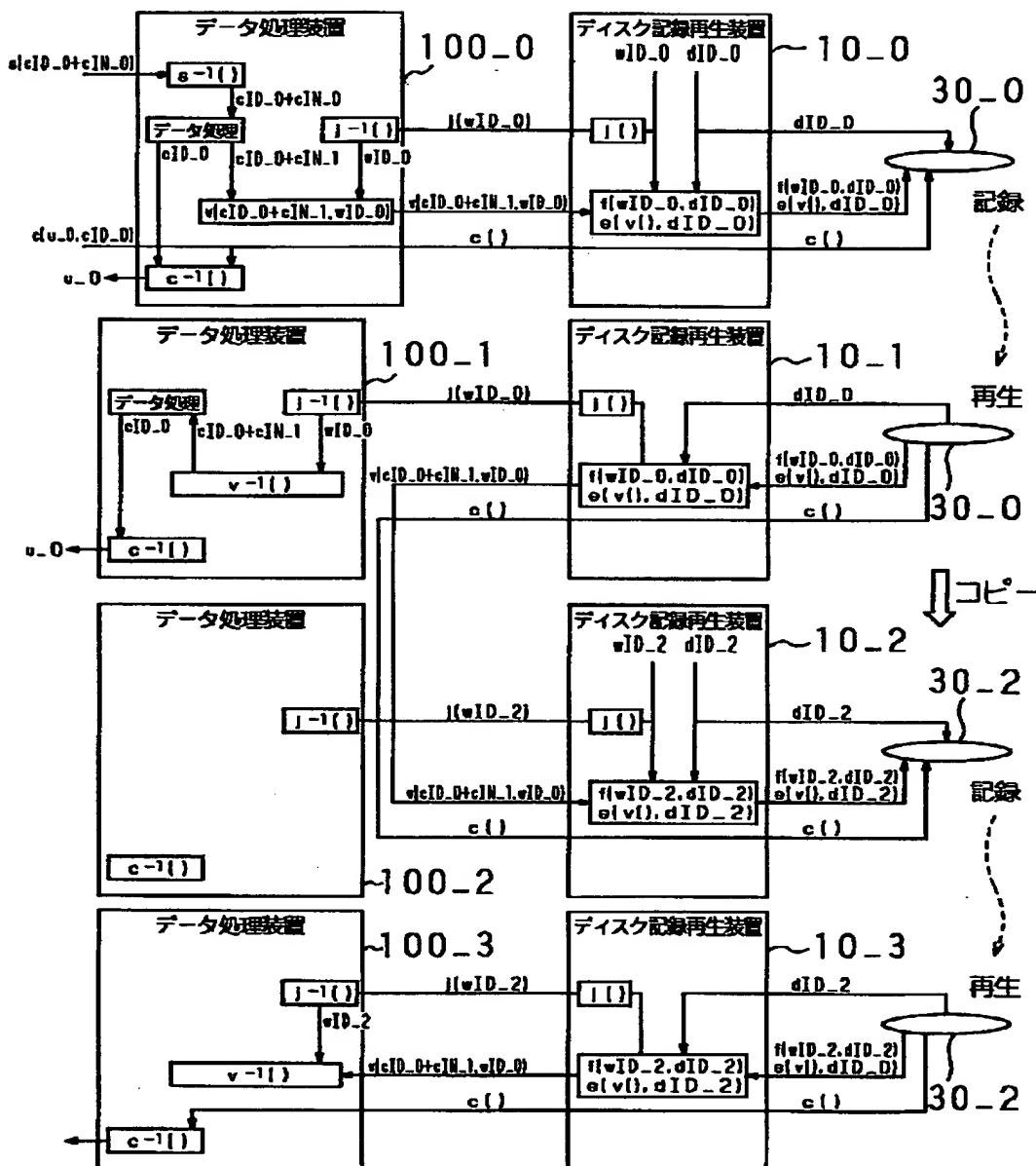
【図1】



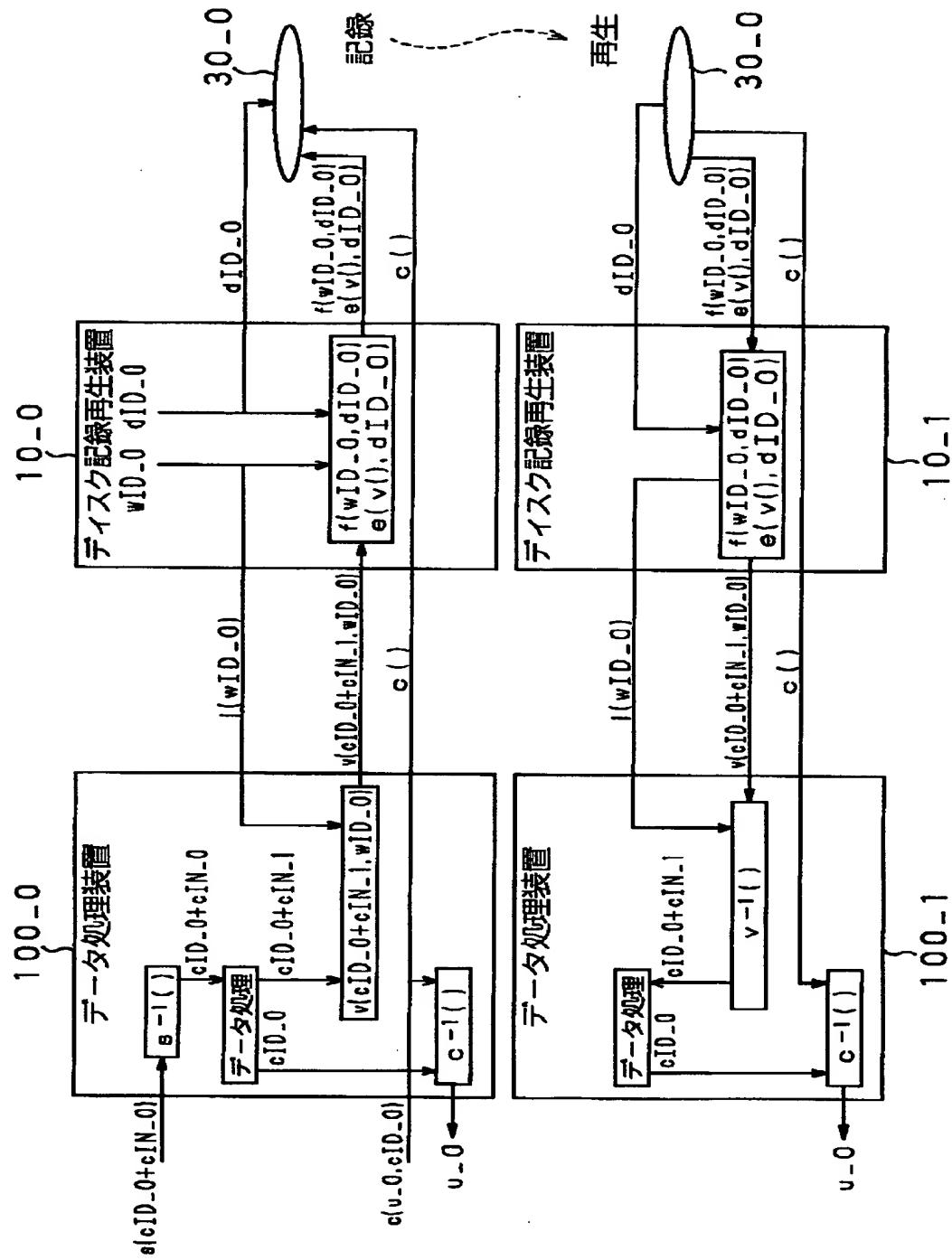
【図2】



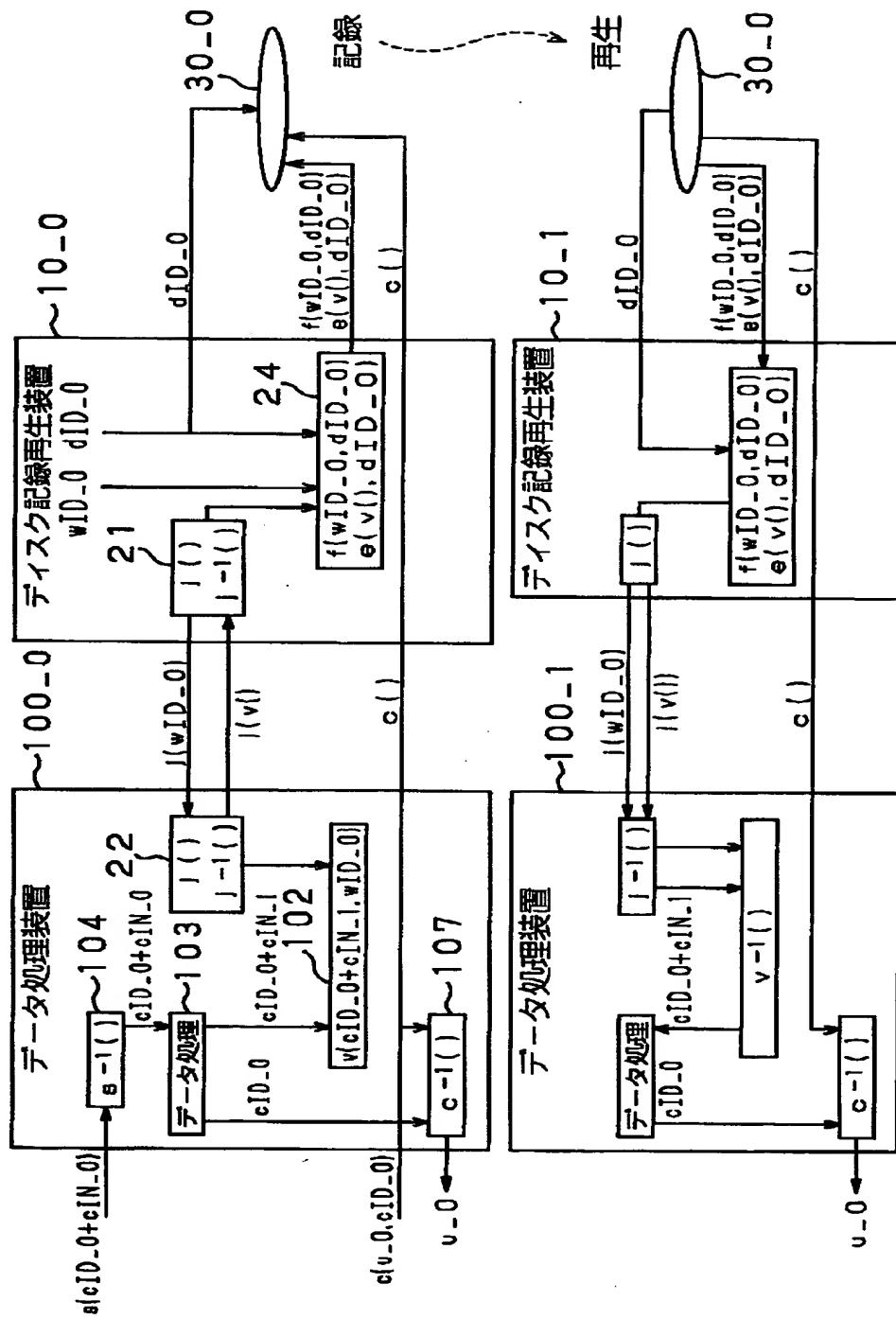
【図3】



【図4】



【図5】



【書類名】 要約書

【要約】

【課題】 データ処理装置とディスク記録再生装置との間で伝送される信号がモニタされても暗号化されたコンテンツデータのコピー保護が有効に行われるようになる。

【解決手段】 ディスク記録再生装置10の記録ID生成部20にて記録毎に固有の記録IDを生成し、この記録IDをデータ処理装置100の暗号化部102に送って、暗号化コンテンツデータの鍵情報となるコンテンツID及びコピー禁止や制限等を行うためのデータ制御情報を、記録IDによる暗号化の鍵を用いて暗号化する。暗号化されたデータは、I/F101、19を介してディスク記録再生装置10の暗号化部24に送られ、記録IDと共に、ディスクIDを用いた暗号化の鍵により暗号化され、ディスク30に記録される。

【選択図】 図1

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社